IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

CIVIL ACTION NO. 5:15-CV-00077-D

DAVID WOOD, *et al.*, Plaintiffs, v. LENOVO (UNITED STATES) INC. and SUPERFISH, INC., Defendants.	**DEFENDANT LENOVO'S OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION**

Plaintiffs' Motion for Preliminary Injunction [Dkt. 13] ("Motion") asking this Court to mandate preliminary injunctive relief should be denied. Seeking to act both individually and on behalf of a putative class, Plaintiffs want to change, not maintain, the status quo: They seek an immediate order requiring Defendant Lenovo (United States) Inc. ("Lenovo") to provide notice to a putative class that has not been certified, without a showing of imminent irreparable harm, and in reliance primarily on third-party hearsay press releases and media publications.

Tellingly, although 25 similar complaints have been filed across the United States, no other set of plaintiffs in any of the other actions is seeking a preliminary injunction. Just as tellingly, in filings before the Judicial Panel for Multi-District Litigation ("JPML"), Plaintiffs' counsel point to their filing of this Motion as one reason why these class actions should be transferred to this District rather than others.[1] The Motion is primarily an attempt by a single set of plaintiffs' counsel to distinguish themselves from the other cases pending a venue decision by the JPML, in an effort to assume the lead role in nationwide litigation. Plaintiffs' Motion is procedural posturing.

Most importantly, Plaintiffs have both the facts and the law wrong: As one example only, the Superfish Visual Discovery software ("Software") has never allowed Lenovo to intercept, store, use

[1] Plaintiffs cite to the pending Motions to Expedite Discovery and for Preliminary Injunction to set themselves apart for the JPML. *See* The *Wood* Pls.' Interested Party Resp. in Supp. of Mot. for Transfer to the E.D.N.C., Dkt. 19, MDL No. 2624 at 8 (citing their pending Motions, Plaintiffs assert: "The *Wood* Action Is The Most Procedurally Advanced").

or transfer consumers' confidential personally identifiable information ("PII"). Plaintiffs also incorrectly assert Lenovo has "simply relied on certain news media" to provide "half-hearted notice" to consumers of issues with the Software. As detailed below, Lenovo has made extensive and extraordinary efforts to address any issues relating to the Software. Nor are Plaintiffs able to show a clear and convincing likelihood of success on the merits. In fact, despite alleging a myriad of federal and state law claims in their Amended Complaint, Plaintiffs have only attempted to meet their burden on two categories of their claims, and in those arguments, they are wrong on the law and fall well short of their burden.

In effect, Plaintiffs portray this as a data breach case where PII has been or will be hacked. Plaintiffs, however, cannot and have not shown any evidence that their Lenovo devices are at risk of causing them or others imminent harm. For these and all of the reasons set forth in this Opposition, this Court should deny Plaintiffs' request for mandatory injunctive relief.

STATEMENT OF THE FACTS

Overview

Plaintiffs allege that between September 2014 and February 2015, Lenovo sold certain laptops ("Affected Machines") which came pre-installed with the Software. Am. Compl. ¶ 2. Their Motion is premised largely on the following grossly flawed and erroneous supposition:

> Until Lenovo gives proper notice, unsuspecting Class members will continue to use the Affected Machines to shop, bank, file taxes, communicate with medical personnel and send other secure confidential communications to financial institutions, insurers, government agencies and attorneys, among others. Their communications will be intercepted by the Superfish Software – in violation of federal and state law – and will be easily available to any third-party hacker who cares to obtain them.

Pls.' Mem. in Supp. of Mot. For Prelim. Inj. [Dkt. 14] ("Mem.") at 12. This and similar allegations by the Plaintiffs ignore the following facts:

- The named Plaintiffs do not allege, state, or provide any evidence that by using the Software, any hackers have actually accessed and/or compromised their PII.

- The Software has never been able to intercept, receive, store, or transfer any PII, including user identity data, passwords or financial information.

- The HTTPS site functionality on which Plaintiffs' claims are based was disabled in September 2014, and since that time, when the Software detects that a user is running on an HTTPS page, the Software does not function.

- A new version of the Software ("Version 1.0.0.5") was shipped on Lenovo devices beginning in November 2014. Version 1.0.0.5 not only lacked any HTTPS functionality, it also lacked a self-signed root certificate. All but one of the Plaintiffs purchased a Lenovo device after this new version had been installed.

- While Lenovo has acknowledged publicly that it was a mistake to pre-load the Software, Lenovo did not design or produce the Software and did not know about a real security issue until February 19, 2015.

- When Lenovo learned of that security issue, it acted swiftly and decisively to remove the Software from Affected Machines. Lenovo has made extensive efforts to notify as many potentially affected persons as possible of the issues with the Software and to remove the Software from the Affected Machines.

- Approximately 80-90% of all Affected Machines have already had the Software removed. Even if Lenovo were to use its best efforts, it is highly unlikely that it would ever be able to identify and individually contact the remaining affected individuals.

- There is no imminent threat. There has not been, nor will there likely ever be, a wide-scale hacking incident resulting from the Software.

The Software And How It Worked – No Personal Data Received

When Lenovo first encountered Superfish, Inc. ("Superfish") in the spring of 2014, Superfish was a highly regarded company – "once named America's fastest-growing software start-up."[2] Its visual search technology has been described by industry experts as "the next big thing in online shopping," "probably one of the best technologies that's out there," and "a powerful tool for a lot of things."[3]

[2] Nicole Perlroth, "How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs," *New York Times*, March 1, 2015 (fn. 13 to Amended Complaint and attached to Lenovo's Appendix of Materials Cited in Opposition to Motion for Preliminary Injunction and Opposition to Motion for Expedited Discovery ("Appx.") as Ex. L). The Declaration of Amanda Ray attests that each of the Exhibits D-S in the Appendix is a true and accurate copy of the document.

[3] "Superfish Points Fingers Over Ad Software Security Flaws" *New York Times*, Feb. 21, 2015 (fn. 51 to Amended Complaint; Appx. Ex. N).

The Software provided visual searching of similar items. When a user's mouse pointer hovered over an image of a vase on a shopping website, the Software would produce images of similar vases on other websites, including their prices. Superfish had "partnerships with 100,000 retailers."[4] Lenovo preloaded the Software onto several models of IdeaPad laptops beginning in September 2014. When a user first visited a shopping website, s/he would be presented with an "opt out" opportunity.[5] If the user opted out, the Software would then be inoperable on that computer, though it still resided there.[6] Users also had the option to uninstall the Software.[7]

Importantly, the Software did not store or retain any PII from users' computers.[8] Instead, the Software only received image information: "It does not profile nor monitor user behavior. It does not record user information. It does not know who the user is. Users are neither tracked nor re-targeted. Every session is independent."[9] In any event, Lenovo received no user information via the Software.[10]

Changes To the Software Functionality In The Fall Of 2014

On September 24, 2014, shortly after the first shipment of Lenovo computers preloaded with the Software, Lenovo asked Superfish to disable the HTTPS functionality of the Software at the server level.[11] HTTPS websites utilize a security feature that regular HTTP (Hypertext Transfer Protocol) websites do not have. Most banking websites, for example, are HTTPS because private financial information is transferred. After September 24, when a Lenovo customer accessed an HTTPS website, such as a bank, the Software did not function.[12]

---

[4] Appx. Ex. L
[5] "Updated Lenovo Statement on Superfish," Feb. 20, 2015 (fn. 35 to Amended Complaint and Appx. Ex. R) ("users are given a choice whether or not to use the product"); *see also* Screenshot of Opt Out Message (Appx. Ex. M)
[6] *Id*.
[7] *Id*.
[8] Declaration of Ronen Daniel ("Daniel Decl.") at ¶¶ 3-4; *see also* Appx. Ex. L ("Mr. Pinhas [CEO of Superfish] maintains that Superfish does not log any personal information on its servers").
[9] Appx. Ex. R; *see also* Daniel Decl. at ¶¶ 3-4.
[10] Declaration of Ed Grant ("Grant Decl.") at ¶3.
[11] Grant Decl. at ¶4.
[12] *Id*.

After the servers were turned off for HTTPS, Superfish designed Version 1.0.0.5.[13] The new version was placed onto Lenovo computers beginning in November 2014. Version 1.0.0.5 did not operate on HTTPS websites (which had already been removed at the server side), and it did not contain self-signed root certificates. In other words, computers shipped with Version 1.0.0.5 did not contain the security vulnerability that the original version contained, and which Lenovo only learned of on February 19, 2015.[14] Notably, of the 11 named Plaintiffs in this action, all but one purchased their Lenovo device on or after November 26, 2014. Am. Compl. ¶¶ 16-26. Thus all but one of the Plaintiffs purchased a device shipped with Version 1.0.0.5, which had no HTTPS functionality and no self-signed root certificates.

January 2015 – Superfish Servers Shut Off For Good

Lenovo received complaints about unwelcome user experiences with the Software, and decided in January 2015 to take three immediate actions: (1) have Superfish disable all server side interactions on all Lenovo products so that the Software was no longer active (effectively disabling the Software for all Lenovo products on the market); (2) remove all the preloads of the Software on all Lenovo products which had not yet been shipped; and (3) halt the preloads of the Software on all future Lenovo products.[15] Thus, the servers have been completely disabled – and the Software has been inoperable – on Lenovo computers since January.[16]

February 19, 2015 – Lenovo Learns of Security Issue

On February 19, 2015, Lenovo learned that the original version of the Software included "a self-signed root certificate in the local trusted CA store."[17] By itself, this would not raise a significant security concern, but it was also discovered that a software vendor downstream to Superfish (Komodia) had encrypted the certificate with an easily-deciphered password – "komodia" – that was

[13] *Id*. at ¶5.
[14] *Id*.
[15] "Lenovo Security Advisory LEN-2015-010" (fn. 7 to Amended Complaint and Appx. Ex. I).
[16] The servers had already been disabled for HTTPS functionality since September 2014. Grant Decl. at ¶4.
[17] Appx. Ex. I; *see also* Grant Decl. ¶5.

the same for all users and websites. This facet of the original Software created a remote vulnerability to "hacking" into individual affected computers. This vulnerability is not present in Version 1.0.0.5 installed beginning in November 2014.[18]

Lenovo's Acts To Remove the Software

When Lenovo discovered the security issue on February 19,[19] it "moved as swiftly and decisively as we can based on what we now know."[20] In addition to its prior actions – disabling the Superfish servers, eliminating any HTTPS functionality, releasing Version 1.0.0.5, and no longer shipping devices with the Software – Lenovo undertook to close the security vulnerability of the Software. Specifically Lenovo:

1. Issued public statements, website notices, links on Twitter, gave media interviews, and got the word out.[21]

2. Developed and provided a free uninstall program to remove the Software and all remnants/certificates.[22]

3. Worked with leading anti-virus program vendor McAfee to remove the Software completely. Lenovo IdeaPad laptops are shipped with a trial version of McAfee; Lenovo also offered a free 6-month subscription or extension of the McAfee anti-virus program.[23]

---

[18] Grant Decl. ¶5.

[19] Lenovo's discovery of the security concern on February 19, 2015 is seen in Lenovo's statements the next day, such as the "Updated Lenovo Statement on Superfish," Feb. 20, 2015 (Appx. Ex. R) ("we did not know about this potential security vulnerability until yesterday").

[20] *Id.*; *see also* "Lenovo Statement on Superfish," Feb. 19, 2015, Lenovo website, http://news.lenovo.com/article_display.cfm?article_id=1929 (App. Ex. J).

[21] In addition to various Lenovo statements cited above, *see also* Jordan Robertson, "Lenovo Apologizes After It 'Messed Up' With Tracking Software," *Bloomberg*, Feb. 19, 2015 (fn. 2 to Amended Complaint and Appx. Ex. H); Nicole Perlroth, "Lenovo's Chief Technology Officer discusses the Superfish Adware Fiasco," *New York Times*, Feb. 24, 2015 (fn. 26 to Amended Complaint and Appx. Ex. K).

[22] Ex. A to Plaintiffs' Preliminary Injunction Motion; "Superfish Uninstall Instructions," http://support.lenovo.com/us/en/product_security/superfish_uninstall (Appx. Ex. O); Connecticut Attorney General Press Release "AG Jepsen Opens Inquiry Into Lenovo, Superfish Privacy and Security Concerns," Mar. 2, 2015 (fn. 14 to Amended Complaint and Appx. Ex. E) (stating that Lenovo "created a fix to purge the software and the certificate from computer systems"); Appx. Exs. I and R.

[23] Appx. Ex. R; "Information on Free McAfee Subscription for Lenovo Customers with Superfish Preload," Lenovo website, http://support.lenovo.com/us/en/mcafeesubscription (Appx. Ex. G); "Update on Free McAfee Subscription for Lenovo Customers with Superfish Pre-load," Mar. 6, 2015, Lenovo website, http://news.lenovo.com/article_display.cfm?article_id=1945 (Appx. Ex. Q); "Virus Profile: BackDoor-FCNC," Feb. 22, 2015, McAfee website, http://home.mcafee.com/virusinfo/virusprofile.aspx?key=9593355 (Appx. Ex. S).

4. Worked with Microsoft to remove the Software via Windows Defender, a free program that kicks in when no other anti-virus software is operating.[24]

5. Worked with Symantec, the maker of Norton AntiVirus, another leading anti-virus program, to add the Software removal to Symantec's functionality.[25]

6. Issued an "Important Security Message" to users directly via the Lenovo Messenger advisory tool.[26] The message went out on March 21, 2015 to users whose computers still contained the Software. The message included instructions on how to manually or automatically remove the Software.[27]

In addition to these actions taken by Lenovo, others have also helped spread the word and eliminate the Software from Lenovo computers. Third-parties heavily publicized the security vulnerability and instructions on how to remove the Software.[28]

Lenovo's actions, as described even in documents cited in the Amended Complaint, "solved the security problem."[29] "These actions have already started and will automatically fix [through anti-virus programs like McAfee, Norton and Windows Defender] the vulnerability even for users who are not currently aware of the problem."[30]

---

[24] Appx. Ex. R; Brad Chacos, "Bravo! Windows Defender, McAfee updates fully remove Lenovo's dangerous Superfish adware," *PC Magazine* Feb. 20, 2015, http://www.pcworld.com/article/2886827/bravo-windows-defender-update-fully-removes-lenovos-dangerous-superfish-malware.html (Appx. Ex. D).

[25] "Symantec Security Response: Adware. Superfish," http://www.symantec.com/security_response/print_writeup.jsp?docid=2015-022009-1243-99 (Appx. Ex. P) ("Symantec detects SuperFish as Adware.SuperFish and remediates the application by removing the application and its associated files. It also removes the SuperFish root certificate from the Windows Certificate Store.").

[26] After March 21, 2015, the first time a user of an Affected Machine rebooted the machine, the Lenovo advisory tool checked the machine for any sign of the Software. If the Software is on the machine, the tool provides the "Important Security Message" with a dialog box and link to a Lenovo webpage which tells the user to remove the Software either by clicking on the Lenovo removal tool or by following the manual uninstall instructions. The Lenovo Messenger advisory tool will be seen by all using an Affected Machine with the Software on it who reboot after March 21 and who have not turned off the Messenger feature. Declaration of Jim Hunt ("Hunt Decl.") at ¶3.

[27] Hunt Decl. ¶3; *see also* "Important Security Message From Lenovo," Lenovo website, http://support.lenovo.com/en/product_security/superfish/Messenger (App. Ex. F).

[28] See the numerous articles cited in the Amended Complaint, including those at fns. 2-5, 8, 11-14, 23, 26, 27, 34, 36, 41, 43 and 51.

[29] App. Ex. K.

[30] App. Ex. R.

Plaintiffs' Factual Mischaracterizations and Errors

Plaintiffs' Motion is premised on allegations that don't square with the facts. The Motion relies more on hyperbole than truth, is contrary to the very documents Plaintiffs cite, and relies on third-party information rather than a correct understanding of how the Software works.

As one example of Plaintiffs' hyperbole, citing no support whatsoever, Plaintiffs assert that "Defendants Lenovo and Superfish, Inc. ('Superfish') intentionally created an ongoing cybersecurity disaster." Mem. at 2. There is no cybersecurity "disaster" here. To Lenovo's knowledge, no criminal has hacked or otherwise exploited a security vulnerability in the Software to obtain any named Plaintiffs' PII.

Nor do Plaintiffs understand the limited, very narrow vulnerability that occurred. While the Software created a temporary vulnerability for individual computers, a criminal hacker wanting to steal PII could do so only with one computer at a time, under exceptional circumstances,[31] using an early version of the Software. Not one of the 11 named plaintiffs alleges that s/he was hacked. No evidence exists that the Plaintiffs' PII has been intercepted or stolen through the use of the Software, even on the September 2014 devices with the older version of the Software still operating. In other words, for over six months this vulnerability has existed – yet these Plaintiffs cannot say that any of their PII has been compromised.

Nor is there any basis for the claim that Lenovo "intentionally" caused a security issue. Again, Lenovo did not discover a real security risk until February 19, 2015. App. Ex. R; Grant Decl. ¶ 5. Surprised and dismayed, it took immediate action to remove the threat. *See* notes 21-27 *supra*.

[31] In order for someone to be hacked using the Software, the following must occur fortuitously and simultaneously: (1) the computer must have the Software on board, i.e., not uninstalled by one of the many manual and automatic mechanisms; (2) the Software version on board must be the original version, not Version 1.0.0.5; (3) the user must be connected to the internet; (4) the internet connection must be on an unsecure network – such as at a coffee shop; (5) a criminal must also be present at the same place and time; (6) the criminal must have the desire to violate the law; and (7) the criminal must know how to hack via the Software and have the time to do it.

Plaintiffs incorrectly assert that "[o]nly Class members who know of the risk, however, will be able to remove the Software." Mem. at 11. This is untrue. By far the most effective removal of the Software is by programs such as McAfee and Norton that work automatically, "even for users who are not currently aware of the problem."[32]

Similarly, Plaintiffs contend that Lenovo "has not even attempted to directly contact affected customers, either by mail or electronic means." This, too, is false. Lenovo has taken aggressive, decisive, creative action on a number of fronts – far more than what Plaintiffs suggest. Not only is this response anything but "half-hearted," but the complete absence of harm demonstrates *that such measures are working.*

ARGUMENT

I. GRANTING MANDATORY INJUNCTIVE RELIEF IS DISFAVORED AND REQUIRES A STRONG SHOWING OF IMMINENT HARM AND A CLEAR AND CONVINCING PROBABILITY OF SUCCESS ON THE MERITS.

With their Motion, Plaintiffs do not seek to maintain the status quo, but rather ask this Court to intervene immediately by ordering Lenovo to take affirmative actions to identify users of the Affected Machines and then to individually notify each user of the issues with the Software through mail and e-mail. Plaintiffs have failed to demonstrate their entitlement to a preliminary injunction of any sort, much less satisfied the exceptionally high standard required in order obtain a mandatory injunction. *See League of Women Voters of N.C. v. N.C.*, 769 F.3d 224, 235 (4th Cir. 2014) (preliminary mandatory relief "in any circumstance is disfavored"); *Rouser v. White*, 707 F. Supp. 2d 1055, 1061 (E.D. Cal. 2010) (mandatory injunctions will only be granted if "extreme or very serious damage will result"); *Burgos v. Univ. of Cent. Fl. Bd. of Tr.*, 283 F. Supp. 2d 1268, 1271 (M.D. Fla. 2003) (mandatory preliminary injunction requiring defendant to take affirmative action is proper only in "rare instances"). To put it simply, Plaintiffs cannot show that irreparable injury will occur if the injunction does not ensue, cannot show a clear and convincing probability of success on any of their

[32] *See supra* notes 23, 25-27.

claims, cannot demonstrate that the balance of equities favors Plaintiffs, and cannot point to any applicable case law where a **mandatory** injunction was issued under remotely similar facts.

For a court to grant a preliminary injunction, it must comply with the procedural requirements of Rule 65. *See* Fed. R. Civ. P. 65. Specifically, to prevail on a motion for a preliminary injunction, a plaintiff must show that (1) he is likely to succeed on the merits; (2) he is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in his favor; **and** (4) an injunction is in the public interest. *Real Truth About Obama, Inc. v. FEC*, 575 F.3d 342, 346 (4th Cir. 2009) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)); *see also Dewhurst v. Century Aluminum Co.*, 649 F.3d 287, 290 (4th Cir. 2011). The "moving party ***must independently satisfy all four requirements*** for a preliminary injunction, and the district court should not balance the four factors." *CWCapital Asset Mgmt., LLC v. Burcam Capital II, LLC*, No. 5:13–CV–278–F, 2013 WL 3288092 at *6 (E.D.N.C. June 28, 2013) (emphasis added) (citing *Real Truth About Obama, Inc.*, 575 F.3d at 346-47 and *Winter*, 555 U.S. at 22).

An even more stringent standard applies when seeking a mandatory injunction: a plaintiff must demonstrate "a ***strong showing of irreparable injury***" and a "***clear and convincing probability of success***." *Cornwell v. Sachs*, 99 F. Supp. 2d 695, 704 (E.D. Va. 2000) (citing *Tiffany v. Forbes Custom Boats, Inc.*, No. 91-3001, 959 F.2d 232 (4th Cir. 1992)). "[I]f there is doubt as to the probability of plaintiff's ultimate success," a request for preliminary mandatory relief "must be denied." *Id.*; *see also Wetzel v. Edwards*, 635 F.2d 283, 286 (4th Cir. 1980) (Mandatory injunctions "normally should be granted only in those circumstances when the exigencies of the situation demand such relief."); *In re Microsoft Corp. Antitrust Litig.*, 333 F.3d 517, 526 (4th Cir. 2003), *abrogation on other grounds recognized in Bethesda Softworks, LLC v. Interplay Entm't Corp.*, 452 Fed. Appx. 351, 353-54 (4th Cir. 2011); *NAACP-Greensboro Branch v. Guilford Cnty. Bd. of Elections*, 858 F. Supp. 2d 516, 530 (M.D.N.C. 2012).

Plaintiffs have failed to carry their burden with respect to any of these four requirements.

II. PLAINTIFFS CANNOT MAKE A STRONG SHOWING OF IRREPARABLE HARM ABSENT AN INJUNCTION.

Plaintiffs seeking a preliminary injunction must "demonstrate that irreparable injury is *likely* in the absence of an injunction"; the mere "possibility" of irreparable harm is not sufficient. *Winter*, 555 U.S. at 22; *Real Truth About Obama, Inc*., 575 F.3d at 347 (plaintiff must make a "clear showing that it is likely to be irreparably harmed absent preliminary relief"; a "possibility" of irreparable injury is not enough). The threshold is even higher in this case: "[w]here, as here, mandatory relief is sought, as distinguished from the maintenance of the status quo, ***a strong showing of irreparable injury must be made***, since relief changing the status quo is not favored unless the facts and law clearly support the moving party." *Tiffany*, 959 F.2d at *6.

At this stage, "irreparable harm consists of harm that could not be sufficiently compensated by money damages or avoided by a later decision on the merits." *MicroAire Surgical Instruments, LLC v. Arthrex, Inc*., 726 F. Supp. 2d 604, 634 (W.D. Va. 2010).

> The key word in this consideration is *irreparable*. Mere injuries, however substantial, in terms of money, time and energy necessarily expended in the absence of a stay, are not enough. The possibility that adequate compensatory or other corrective relief will be available at a later date, in the ordinary course of litigation, weighs heavily against a claim of irreparable harm.

Sampson v. Murray, 415 U.S. 61, 90 (1974). Plaintiffs simply have not, and cannot meet, this heavy burden.

A. Plaintiffs Have Not Alleged Any Actual Injury, Only an Inchoate and Speculative "Risk" of Loss, Which is Not Sufficient to Meet the Irreparable Harm Prong.

To date, not one of the 11 named plaintiffs has asserted that s/he has been hacked or sustained any actual, economic damages. In fact, the only "irreparable harm" that Plaintiffs even attempt to allege *may* occur is a:

> serious risk [to] unsuspecting Class members [who] continue to use the Affected Machines to shop, bank, file taxes, communicate with medical personnel and send other secure confidential communications

> to financial institutions, insurers, government agencies, and attorneys, among others [that their] communications will be intercepted by the Superfish Software . . . and will be easily available to any third-party hacker who cares to obtain them.

Mem. at 12. In essence, Plaintiffs assert that the Software would allow any "third-party hacker who cares" to "hijack" intercepted confidential communications on the Affected Machines and then the "malicious" third-party may use the Software's trusted certificate to conceal his own intercepted communications and spoofed certificates to perform unspecified nefarious acts. Mem. at 2, 5, 12.

Plaintiffs' allegations of risk of harm are completely inaccurate. Not one single Plaintiff in this action has alleged that his Affected Machine was hacked, his PII was stolen, or the information was used to cause harm. Plaintiffs are also wrong about the potential future risk. The only possibility of any security vulnerability rests on a long chain of speculative events:

- A Plaintiff must be using an Affected Machine with a version of the Software pre-dating Version 1.0.0.5,
- On an unsecure network (such as at an airport or coffee shop),
- With a criminal present at the same time and location,
- The criminal must know the Software is running on the Affected Machine,
- The criminal must know how to hack the Software and obtain the private encryption key,
- The criminal must hack the Plaintiff's machine and intercept Plaintiff's PII, and
- The criminal must then use the information to cause harm.

This daisy chain sequence of events has not occurred, nor have Plaintiffs shown it will imminently occur. Plaintiffs clearly fall far short of the required "strong showing" of "imminent" and "irreparable" harm. **"[S]peculation that such losses might occur**, without more, [does not] warrant[] a finding of irreparable harm and the issuance of a preliminary injunction." *MicroAire Surgical Instruments*, 726 F. Supp. 2d at 635 (emphasis added) (internal citations and quotations omitted). A plaintiff "**must show that it will experience a loss**, at which point, a showing that

monetary damages are difficult to ascertain or inadequate generally supports a finding of irreparable injury." *Id.* at 639 (emphasis added). Speculative allegations about what is possible are insufficient. *See id.* This is particularly true where, as here, the Software has been in use by hundreds of thousands of consumers over six months and none of the Plaintiffs here have alleged that the very hypothetical they pose has in fact occurred.

Courts across the country have found similar "increased security risks" to be too speculative to even support the plaintiff's standing (discussed below in Section III.A), much less an imminent and "strong showing of irreparable injury." *See, e.g., Clapper v. Amnesty Int'l USA*, __ U.S. __, 133 S. Ct. 1138, 1147 (2013); *Katz v. Pershing*, 672 F.3d 64, 79-80 (1st Cir. 2012); *Remijas v. Neiman Marcus Grp., LLC*, No. 14-C-1735, 2014 WL 4627893 at *4 (N.D. Ill. Sept. 16, 2014); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 875-76 (N.D. Ill. Mar. 12, 2014).

Plaintiffs also fail to address why any potential damages could not be compensated by money. Plaintiffs themselves specifically note that in 2014, the "average identity fraud victim incurred a mean of $365 in costs as a result of the fraud." Mem. at 12. Plaintiffs have not, and cannot, explain why money would fail to compensate potential victims of identity theft here.

B. Plaintiffs Have Failed To Show That The Individual Notice They Request Will Be More Effective To Prevent Harm Than The Efforts Lenovo Has Already Taken.

Plaintiffs seek to require Lenovo to individually notify each purchaser of an Affected Machine of the issues with the Software. Mem. at 11-12. Plaintiffs, however, have failed to demonstrate how the relief they request would provide any better notice than the efforts Lenovo continues to take voluntarily—or how the failure to provide the notice that Plaintiffs prefer would result in irreparable harm to consumers. Instead, Plaintiffs ask the Court to tinker with Lenovo's efforts without any demonstration that the relief they request would result in even a marginally better notice to consumers. At best Plaintiffs simply make generalized, derogatory comments about Lenovo's actions without detailing specific, demonstrable facts that the injunction they seek is

necessary, reasonable, or likely to effectively avoid any harm that is real, imminent and irreparable. Without such evidence, Plaintiffs have failed to demonstrate a strong showing of irreparable harm "in the absence of the injunctive relief requested."

Although it is impossible for Lenovo to provide individual notice to all users with an Affected Machine because no one maintains such a list, Lenovo has gone to extensive efforts to notify as many as possible; in fact, the Lenovo Messenger advisory tool sent notice to all users even though Lenovo does not know who those users are. Hunt Decl. at ¶3. Other efforts include all of the following:

- Issuing public statements, website notices, and links on Twitter containing detailed information about the issues with the Software;[33]
- Writing code for a program to remove the Software and all remnants/certificates, and making that code available to everyone for free;[34]
- Working with McAfee and Symantec and other anti-virus programs to remove the Software completely and automatically from Affected Machines;[35]
- Working with Microsoft to remove the Software completely via the free Windows Defender when other anti-virus programs are not operating;[36]
- Providing user technical support for removal online and by phone;
- Issuing an "Important Security Message" to users directly via the Lenovo Messenger advisory tool. The message went out on March 21 to users whose computers still contained the Software. The message included instructions on how to manually or automatically remove the Software.[37]

Lenovo's extensive efforts to reach affected users have been very successful. Lenovo's records indicate that 80-90% of the Affected Machines have already removed the Software.[38] Because it is impossible for Lenovo to provide notice to all users of Affected Machines, and Lenovo's extensive outreach and notification methods have already been highly successful, Plaintiffs cannot demonstrate irreparable harm will occur unless the Court enters a mandatory injunction.

[33] *See* note 21 *supra*. Plaintiffs further note in their filings that the text of their proposed individual notice comes "verbatim" from Lenovo's website. Mem. at 13.
[34] Hunt Decl. ¶3; *see also* note 22 *supra*.
[35] *See* notes 23 and 25 *supra*.
[36] *See* note 24 *supra*.
[37] Hunt Decl. ¶3; *see also* notes 26 and 27 *supra*.
[38] Hunt Decl. ¶4.

Plaintiffs or the Court could always hypothesize ways to marginally improve notice to affected consumers—but that does not mean that any demonstrated improvement (even if Plaintiffs had shown any, which they have not) is enough for a "strong showing of irreparable harm in the absence of that relief."

Moreover, Plaintiffs fail to cite any case where a court ordered a defendant to provide "better notice" to an uncertified class at a preliminary injunction stage. Instead, Plaintiffs cite three cases in the very specific context of a Rule 23 notification to a class—which took place after certification of a class and entry of a judgment.[39] Mem. at 12. Unlike the relief requested here, class notifications are subject to rigorous rules to ensure that class members are not deprived of their due process rights by being foreclosed from pursuing future actions. *Eisen v. Carlisle and Jacquelin*, 417 U.S. 156, 173 (1974) ("mandatory notice pursuant to subdivision (c)(2) . . . is designed to fulfill requirements of due process to which the class action procedure is of course subject").

Even for notice of class certification pursuant to Rule 23, "courts retain discretion to tailor notice to the relevant circumstances" and the "determination of what efforts to identify and notify are reasonable under the circumstances of the case rests in the discretion of the judge before whom the class action is pending." *Sobel v. Hertz Corp.*, No. 3:06-CV-00545, 2013 WL 5202027 *5 (D. Nev. Sept. 12, 2013). In this case, individual notice to all users with an Affected Machine is impossible. Courts have held in similar situations "where class members cannot be identified for purposes of sending individual notice, notice by publication is sufficient." *Jermyn v. Best Buy Stores, L.P.*, No. 08 Civ. 00214(CM), 2010 WL 5187746 *4 (S.D.N.Y. Dec. 6, 2010) (notice by publication of the class certification sufficient where Best Buy did not maintain a list of affected customers); *see also Mirfashi v. Fleet Mortg. Corp.*, 356 F.3d 781, 786 (7th Cir. 2004); *Greenfield v. Villager Indus., Inc.*, 483 F.2d 824, 830 (3d Cir. 1973).

[39] Plaintiffs' argument here reinforces the likelihood that their Motion is more about advancing a class action prematurely than solving a software security issue.

III. PLAINTIFFS HAVE NOT SHOWN A CLEAR AND CONVINCING PROBABILITY OF SUCCESS ON ANY OF THEIR CLAIMS.

A. Plaintiffs Lack Standing For Claims Based Upon Speculative Future Harm.

Plaintiffs lack the requisite Article III standing to bring their claims because none of them have alleged or produced evidence of facts showing that they have sustained any actual harm, they are threatened with any immediate harm, or such harm can be redressed by a favorable decision. Nor can Plaintiffs cure their lack of standing by bringing claims on behalf of an uncertified class of purported future plaintiffs. The named Plaintiffs must have sustained an injury-in-fact themselves.

Article III of the Constitution limits federal courts' jurisdiction to certain "cases" and "controversies." *Clapper*, 133 S. Ct. at 1146. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Id.* This requires Plaintiffs to demonstrate that: (1) an injury-in-fact that is concrete and particularized and either actual or imminent; (2) the injury is fairly traceable to the challenged action by the Defendants; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Id.* at 1147. It is Plaintiffs' burden to establish Article III standing. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Plaintiffs have failed to meet their burden.

1. Named Plaintiffs Have Not Alleged They Have Sustained Any Actual Harm or Face the Threat of Immediate Harm.

As discussed in Section II.A. *supra*, to date, none of the named Plaintiffs have asserted that, as result of the Software, any of their PII has been acquired by any third-party hacker or used in any way that has caused them actual harm. Rather, Plaintiffs generally assert that they have been "expos[ed] to the inherent risk of theft of their financial, health, or other confidential data." Am. Compl. ¶ 13.[40] Such speculative, future harm is not sufficient to show an injury-in-fact or standing. *Clapper*, 133 S. Ct. at 1147 (citing *Whitmore v. Ark.*, 495 U.S. 149, 158 (1990)).

[40] Additionally, Plaintiffs generally assert that they have lost "time and money" to wipe the Software from their Affected Machines and that they have been forced to monitor their accounts to determine whether third-parties have

Courts have repeatedly held that "increased security risks" theories are not sufficiently "imminent" to support Article III standing. *See, e.g.*, *Katz*, 672 F.3d at 79-80 (plaintiff lacked standing to assert consumer protection claims when claims based on increased risk of a future security breach); *Remijas*, 2014 WL 4627893 at *4 ("[T]he complaint does not adequately allege that the risk of identity theft is sufficiently **imminent** to confer standing."); *Strautins*, 27 F. Supp. 3d at 875 ("To the extent that [plaintiff's claims] are premised on the mere possibility that her [personal information] was stolen and compromised, and a concomitant increase in the risk that she will become a victim of identity theft, [plaintiff's] claim is too speculative to confer Article III standing.").

In *Katz*, the plaintiff accountholder brought a putative class action, asserting that the defendant broker's service storing her PII was inadequate and vulnerable to access by hackers. *Katz*, 672 F.3d at 70. Once she discovered these "inadequacies," plaintiff purchased identity theft insurance and faced an "increased risk" that her PII had been exposed to misappropriation. *Id.* at 78. Plaintiff accordingly asserted that the defendant overcharged for the inadequate service and deprived her of the "benefit of her bargain." *Id.* at 76. Significantly, plaintiff did not allege that her PII had "actually been accessed by an unauthorized user." *Id.* at 79. The First Circuit held that the plaintiff's asserted injuries were insufficient to justify standing:

> Her cause of action rests entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third-party might access her data and then attempt to purloin her identity. The conjectural nature of this hypothesis renders the plaintiff's case readily distinguishable from cases in which confidential data actually has been accessed through a security breach and persons involved in that breach have acted on the ill-gotten information. . . Given the multiple strands of speculation and surmise from which the plaintiff's hypothesis is woven, finding standing in this case would stretch the injury requirement past its breaking point.

---

exploited the Software's vulnerabilities. Am. Compl. ¶ 75. Plaintiffs also assert that they may "have to" pay $120 for another copy of Windows 8.1 to be "completely safe" that they have removed the Software from their machines (but no Plaintiff actually asserts that s/he has already done so). Am. Compl. ¶ 78.

Id. at 79-80.

In *Clapper* the Supreme Court likewise found plaintiff's alleged threatened injury not to be "certainly impending." The plaintiffs alleged that surveillance authorized under the Foreign Intelligence Surveillance Act of 1978 ("FISA") supposedly created an "objectively reasonable likelihood that their communications will be acquired under [FISA] at some point in the future." *Id.* at 1143. They also complained of "costly and burdensome measures to protect the confidentiality of their international communications." *Id.* The Supreme Court, however, held that the plaintiffs lacked standing, and they could not "manufacture standing by choosing to make expenditures based on hypothetical future harm that is certainly not impending." *Id.* The plaintiffs' theory of standing "rested on a highly attenuated chain of possibilities" and did not satisfy the "certainly impending" requirement of a threatened injury. *Clapper*, 133 S. Ct. at 1150. The Court also declined to "abandon [its] usual reluctance to endorse standing theories that rest on the speculation about the decisions of independent actors." *Id.* at 1150.

Plaintiffs' alleged injuries-in-fact are speculative, attenuated and strictly hypothetical based on what some third-party might be able to do under certain particularized and (thus far) non-existent circumstances. As described in footnote 31 *supra*, the only possibility of any security vulnerability rests on a chain of speculative events which have not occurred. Nor have Plaintiffs shown such a chain of events is likely, much less imminent. Consistent with *Clapper* and *Katz*, this highly attenuated and speculative chain of events which are centered on the actions of criminals, does not justify standing.[41]

[41] Additionally, just as the *Clapper* Court was not persuaded by the plaintiffs' attempt to "manufacture standing by choosing to make expenditures based on hypothetical future harm," this Court should not attribute any significance to Plaintiffs' general allegations of "lost time and money" to wipe the Software from their Affected Machines, their time to monitor their accounts for fraudulent activities, a potential future purchase of $120 worth of Windows, or any payment to Lenovo for more than the true market value of the Affected Machine. *Clapper*, 133 S. Ct. at 1143; *see also Katz*, 672 F.3d at 76-78 (not finding any legal significance or injury-in-fact based on the plaintiff's allegation that she sustained injuries by having to purchase identity theft insurance and by paying more for the brokerage fees than the service was worth (essentially, not receiving the benefit of her bargain)).

2. Named Plaintiffs Cannot Assert Claims on Behalf of Unidentified Members of a Purported Class Unless They Have Suffered Directly.

Plaintiffs seek injunctive relief not for themselves, but rather on behalf of unidentified class members who have a pre-Version 1.0.0.5 of the Software running on their Affected Machines and are purportedly unaware of any issues surrounding the Software. In a class action, however, plaintiffs who propose to represent a class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976); *see also Warth v. Selfin*, 422 U.S. 490, 502 (1975); *McKenzie v. City of Chi.*, 118 F.3d 552, 555 (7th Cir. 1997) ("Because a class has not yet been certified, the only interests at stake are those of the named plaintiffs.").

Here, the named Plaintiffs have not alleged or shown any injury-in-fact to themselves. They cannot assert standing on behalf of other unidentified class members, particularly when a class has not yet been certified.

B. PLAINTIFFS HAVE FAILED TO DEMONSTRATE A CLEAR AND CONVINCING LIKELIHOOD OF SUCCESS ON THEIR ECPA CLAIM AND COMPUTER FRAUD AND ABUSE ACT CLAIM (THEIR SO-CALLED "INTERCEPTION BASED CLAIMS").

In their Memorandum, Plaintiffs assert only that they are likely to succeed on their Electronic Communications Privacy Act ("ECPA") Claim and Computer Fraud and Abuse Act ("CFAA") Claim (two of several so-called "interception-based claims") and that they are likely to succeed on their North Carolina Unfair and Deceptive Trade Practices Act ("UDTPA") Claim (one of several so-called "disclosure-based" or "mixed" claims). Mem. at 8-11. While Plaintiffs refer generally to the numerous other state and federal claims asserted in their Amended Complaint, they have not even attempted to meet their burden on those claims of demonstrating a clear and convincing likelihood of success. Accordingly, those claims cannot provide a basis for the relief Plaintiffs seek in this Motion.

[42] *See East Brooks Books, Inc. v. Shelby Cnty. Tenn.*, 588 F.3d 360, 370 (6th Cir. 2009) (finding that, "[w]hile Plaintiff identifies these claims in its initial complaint," arguments in support of injunctive relief relative to these claims were waived where "they are not presented in [plaintiff's] Memorandum in Support of Motion for a Preliminary Injunction"); *see also Thomas & Betts Corp. v. Panduit Corp.*, 138 F.3d 277, 300 n.9 (7th Cir. 1998) (argument not discussed in memorandum of law in support of motion for summary judgment deemed to have been waived).

Though Plaintiffs refer broadly to several "interception-based" claims, the only claims they have relied upon in attempting to meet their burden of showing a clear and convincing likelihood of success on the merits are their claims under the ECPA (Count 2) and the CFAA (Count 3). In support of these "interception-based" claims, Plaintiffs focus on statements in various documents to the effect that the Software "intercepts" web traffic—that is a long way from showing that Lenovo has illegally intercepted anything. Courts have routinely dismissed similar claims. The "wiretap" statutes Plaintiffs invoke simply do not fit.

1. The ECPA (Federal Wiretap Act) Does Not Apply.

The ECPA penalizes anyone who "intentionally intercepts" an "electronic communication." 18 U.S.C. § 2511(1)(a-b). Lenovo did not "intercept" anything. It made computers and shipped them to users. No information was sent to Lenovo's servers when the Software operated. Grant Decl. ¶3; Daniel Decl. ¶3. A device manufacturer who has not itself collected communications is entitled to dismissal of an ECPA claim. *In re Carrier IQ, Inc. Consumer Privacy Litig.*, 2015 U.S. Dist. LEXIS 7123, *103-04 (N.D. Cal. Jan. 21, 2015) (where software installed on smartphones allegedly collected consumer data, device manufacturers were appropriately dismissed because plaintiffs could not allege "that any device manufacturer actually received copies of the plaintiffs' text messages or

[42] Even if the remainder of Plaintiffs' claims were at issue, Plaintiffs cannot show a clear and convincing likelihood of success on the merits on those claims. Should the Court wish to consider the merits of the claims not addressed in Plaintiffs' preliminary injunction briefing, Lenovo would respectfully request permission from the Court to submit additional briefing to demonstrate that those claims are similarly unlikely to succeed on the merits.

internet search inquiries"). The installation of the software was not an "interception," as it could not be said "that the Device Manufacturer themselves 'seized' or 'redirected' any communications themselves." *Id.* at *106. Here, Plaintiffs have not identified any communication they sent that Lenovo acquired in transit.

Nor can Plaintiffs' impute the actions of Superfish or a third-party to Lenovo. There is no secondary, vicarious, or "aiding and abetting" liability under the ECPA. *See, e.g., Carrier IQ, Id.* at *107-10 (courts have "consistently rejected" such liability, citing cases); *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1246 (10th Cir. 2012) (providing means for another party to intercept communications is not covered by ECPA); *Peavy v. WFAA-TV,* 221 F.3d 158, 168-69 (5th Cir. 2000) (same); *In re Toys R Us, Inc., Privacy Litig.*, No. 00-CV-2746, 2001 U.S. Dist. LEXIS 16947, *22 (N.D. Cal. Oct. 9, 2001) (same). Even if the Software intercepted something,[43] Lenovo is not liable.

An "interception" requires an "acquisition" of communications, and Lenovo did not "acquire" Plaintiffs' information. In *Expert Bus. Sys., LLC v. BI4CE, Inc.*, 233 F. Appx. 251, 253 (4th Cir. 2007), the Fourth Circuit rejected an ECPA claim where the defendant installed software on the plaintiff's computers, but did not acquire the plaintiff's "records and data." *See also Halperin v. Int'l Web Servs., LLC*, 2014 U.S. Dist. LEXIS 138600, *1, 15, 18 (N.D. Ill. Sept. 30, 2014) (no ECPA violation where software read URL information and generated pop-up ads when a user's cursor hovered over certain text – "Defendants never 'acquired' the contents of Halperin's communications"). Thus, Plaintiffs cannot prove an ECPA claim against Lenovo.

[43] The ECPA only covers the interception of the "contents" of a communication. Here, even the Software did not acquire the "contents" – it simply analyzed images and URL addresses, Daniel Decl. ¶3, which are not "contents." *See U.S. v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009) (data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute "content" for purposes of the Wiretap Act because such data "contains no information concerning the substance, purport, or meaning of [the] communication") (citation omitted); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105-06 (9th Cir. 2014) (URL and user identity are not "contents" of communications under ECPA).

2. The CFAA (Computer Fraud & Abuse Act) Does Not Apply.

The CFAA penalizes anyone who "intentionally accesses a computer without authorization . . . and thereby obtains [information]." 18 U.S.C. § 1030(a)(2). No action may be brought under the CFAA "for the negligent design or manufacture of computer hardware, computer software, or firmware." 18 U.S.C. § 1030(g).

As a criminal statute, the CFAA is narrowly construed. *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012) (no violation where former employee downloaded confidential information from a company computer). Civil actions are only allowed in very narrow circumstances specified in 18 U.S.C. § 1030(g), none of which exist here.

The CFAA allows a civil suit when the plaintiff alleges and shows "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(g) and (c)(4)(A)(i)(I). Plaintiffs cannot establish any recognizable loss at all, much less the requisite $5,000.

"Loss" under the CFAA means economic loss, but more important:

> It is no surprise that courts interpreting the definition of "loss" sufficient to bring a civil action have done so narrowly given the company that subsection (I) keeps. The definition of "loss" itself makes clear Congress's intent to restrict civil actions under subsection (I) to the traditional computer "hacker" scenario-where the hacker deletes information, infects computers, or crashes networks.

In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1067 (N.D. Cal. 2012) (quoting with approval *AtPac, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010)). Here, Plaintiffs have not pled facts showing any loss, and especially none showing a loss that is subject to the CFAA: No named plaintiff even claims to have been hacked. Damage or loss under the CFAA requires a significant impairment of equipment or systems. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067-68. This only occurs when "the cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service." *Id.*at 1068 (citation omitted); *see also America Online, Inc. v. Nat'l Health Care Disc., Inc.*,

121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) ("when a large volume of [spam] causes slowdowns or diminishes the capacity of AOL to service its customers, an 'impairment' has occurred to the 'availability' of AOL's system"). When the alleged damage is the use of finite memory or battery resources, the CFAA does not apply. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067. Similarly, when the alleged loss is financial or personal information, this is insufficient to trigger the CFAA's civil suit provision. *Bose v. Interclick, Inc.*, No. 10 Civ. 9183 (DAB), 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011); *Volk v. Zeanah*, No. 608CV094, 2010 WL 318261 (S.D. Ga. Jan. 25, 2010); *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).

Not only has no Plaintiff in this action suffered any damage, but none of them has alleged, or can allege, that s/he has met the $5,000 threshold. Plaintiffs' own Memorandum notes that the average loss in the case of a hacking is $365. Mem. at 12. Nor can the injuries of multiple plaintiffs – or unnamed class members – be aggregated to achieve the $5,000 minimum. *Halperin v. Int'l Web Servs., LLC*, No. 13 C 8573, 2014 U.S. Dist. LEXIS 138600, *9-13 (N.D. Ill. Sept. 30, 2014) (rejecting aggregation); *Lyons v. Coxcom, Inc.*, No. 08-CV-02047-H(CAB), 2009 WL 347285, *8 (S.D. Cal. Feb. 6, 2009) (same).

Not only can Plaintiffs not surmount these barriers, it simply is not the case that Lenovo "accessed" Plaintiffs' computers without authorization. The Software was "preloaded" onto the computers, which means it was installed when Lenovo still had control and ownership of the computers. Daniel Decl. ¶2. Lenovo had no further "access" to the computers once they were sold to Plaintiffs. Even if the program's operation could be described as "access" by the Software, Lenovo cannot be held liable for the Software's access or actions. The CFAA, like the ECPA, does not allow vicarious or aiding and abetting liability. *Doe v. Dartmouth-Hitchcock Med. Ctr.*, No. Civ. 00-100-M, 2001 WL 873063 at *5-6 (D.N.H. July 19, 2001) ("Expanding the private cause of action [of the CFAA] to include one for vicarious liability against persons who did not act with criminal intent and

cannot be said to have violated the statute . . . would be entirely inconsistent with the plain language of the statute.").

Plaintiffs therefore have no chance of success on their CFAA claim.

C. PLAINTIFFS HAVE FAILED TO DEMONSTRATE A CLEAR AND CONVINCING LIKELIHOOD OF SUCCESS ON THEIR UNFAIR AND DECEPTIVE TRADE PRACTICE ACT (AND OTHER SO-CALLED "DISCLOSURE BASED") CLAIMS.

Plaintiffs also claim they are likely to succeed on their "UDTPA Claim and Other Disclosure-Based Claims" as well as their "Mixed Claims" because federal courts have purportedly "recognized that a failure to disclose cybersecurity flaws constitutes a breach of state consumer protection laws."[44] Mem. 10. Plaintiffs refer generally to North Carolina's Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, *et seq*., ("UDTPA") and to California's Unfair Competition Law ("UCL"), but do not discuss or cite the standard for these claims, much less how they will likely be successful proving each of the requisite elements. Instead, in support of their request for mandatory injunctive relief, Plaintiffs cite two cases involving security breaches *where hackers actually compromised the plaintiffs' PII* and one case involving a purchase of real estate, none of which remotely apply.

Plaintiffs rely solely on the *Target*, *Adobe*, and *Bear Hollow* cases to argue, incorrectly, that Lenovo violated the UDTPA and other consumer law statutes across the country because it failed to

[44] The first claim Plaintiffs mention in their Amended Complaint is "a nationwide claim under the Racketeer Influenced and Corrupt Organizations Act ('RICO')." Am. Compl. ¶¶ 15, 92-95. Plaintiffs do not discuss their vanguard RICO claim in their Memorandum, nor do they allege or attempt to present any evidence showing a clear and convincing likelihood of success on the merits of this claim. While Plaintiffs reference Superfish's actions in their RICO claim, they do not allege any racketeering activity by Lenovo, except wire and mail fraud. Am. Compl. ¶¶ 92-95. Courts are not inclined to allow RICO claims to proceed based solely on the predicates of wire and mail fraud, as the claim has been articulated here. *Whitehead v. Gateway Chevrolet, et al*., No. 03 C 5684, 2004 WL 316413, *7 (N.D. Ill. Feb.2, 2004) ("The Seventh Circuit has long looked with disfavor upon reliance on mail and wire fraud in order to support a RICO pattern of racketeering activity.") Plaintiffs further allege that "Defendants" (and not Lenovo specifically) committed "Authentication Feature Fraud" and "Trafficking In Counterfeit Labels." If Plaintiffs attempt to base a RICO claim against Lenovo on these two predicate acts, they must provide some evidence that Lenovo actually engaged in them. *See I.S. Joseph, Inc. v. Lauritzen*, 751 F.2d 265, 267 (8th Cir.1984) (RICO "predicate offenses must be strictly construed"); *Federal Deposit Ins. Corp. v. Kerr*, 637 F.Supp. 828, 834 (W.D.N.C.1986) ("general allegations of such a scheme are not sufficient"). They have not done so. The RICO claim is not likely to succeed and cannot form the basis of injunctive relief here.

disclose a "serious cybersecurity flaw." Mem. 8-10. These cases, however, bear little resemblance to the facts at issue here; the procedural postures are significantly different; and they do not address—much less justify—the issuance of a mandatory injunction.

The *Target* and *Adobe* cybersecurity cases examined claims where hackers had actually accessed and compromised the plaintiffs' PII, and the defendant companies failed to timely disclose to the affected consumers serious security flaws known only to the defendants. *See In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, 2014 WL 7192478, *6 (D. Minn. Dec. 18, 2014) (discussing potential duty to disclose under generic consumer unfair protection state statutes); *In re Adobe Sys. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, *20-21 (N.D. Cal. Sept. 4, 2014) (analyzing failure to disclose theory for a UCL claim). Both cases assessed only the sufficiency of the plaintiffs' allegations (not their evidence) on Rule 12 motions to dismiss. Construing those allegations in the light most favorable to the plaintiffs, the courts concluded it was plausible that defendants had a duty to disclose information only it knew, and they denied the motions to dismiss. *See Target*, 2014 WL 7192478 at *6 (plaintiffs asserted Target knew its systems were inadequate to protect credit card numbers and failed to disclose the fact to customers); *Adobe*, 2014 WL 4379916 at *21-22 (defendant knew its specific security shortcomings fell well below industry standards and failed to disclose it to customers).

First, the sparse "evidence" provided with Plaintiffs' Motion presents a vastly different context. No Plaintiff in this action has alleged that a hacker has accessed and compromised PII as a result of the Software. *Contrast* Mem. at 12 (asserting "serious risk" of future hacking) *with Target*, 2014 WL 7192478 at *1 (concerning "one of the largest breaches of payment-card security in the United States retail history [affecting] approximately 110 million customers") and *Adobe*, 2014 WL 4379916 at *21-22 (where hackers accessed the PII of "at least 38 million customers"). Nor have Plaintiffs come forward with *any* evidence to establish that such a hack is imminent.

Second, Plaintiffs have failed to establish facts that Lenovo had a duty to disclose that would give rise to a UDTP claim. Under North Carolina law, a duty to disclose arises: (1) where the parties to the transaction are in a fiduciary relationship; (2) are negotiating at arms' length and one of them takes affirmative steps to conceal material facts from the other; or (3) "where one party has knowledge of a latent defect in the subject matter of the negotiations about which the other party is both ignorant and unable to discover through reasonable diligence." *Harton v. Harton*, 81 N.C. App. 295, 297, 344 S.E.2d 117, 119 (1986); *see also Adobe*, 2014 WL 4379916 at *20 (noting similar circumstances for when a duty to disclose arises under California law). Plaintiffs have shown no such circumstances. Unlike *Target* and *Adobe*, no evidence of record demonstrates that Lenovo knew of a "serious cybersecurity flaw" prior to February 19, 2015 and purposefully failed to disclose that information. Grant Decl. at ¶ 5. Rather, the evidence shows the opposite: as soon as Lenovo became aware of the "serious" flaw, it acted to disclose the information publicly in many different media. *See* notes 21-27 *supra*.

Third, the courts in *Target* and *Adobe* did not evaluate whether plaintiffs had a clear and convincing likelihood of success on the merits. Rather, viewing the allegations in the light most favorable to the plaintiffs, those courts evaluated only whether the consumer protection claims were sufficiently plausible to survive a motion to dismiss.[45] Here, Plaintiffs must actually prove more to meet their heightened burden of showing a clear and convincing likelihood of success. Plaintiffs have not even alleged facts as to unfair, immoral, or deceptive acts that would violate the UDTPA, much less proven any such facts. *AMEC Env't & Infrastructure, Inc., v. Structural Assoc., Inc.*, No. 7:13–CV–21–BO, 2015 WL 1000766 at *7-8 (E.D.N.C. March 5, 2015) (granting summary judgment in

[45] Additionally, the *Bear Hollow, L.L.C. v. Moberk, L.L.C.*, N0. 5:05-CV-210, 2006 WL 1642126, *1, 7-8 (W.D.N.C. June 2, 2006) case fails to support Plaintiffs' failure to disclose theory. In *Bear Hollow*, the plaintiffs alleged that a real estate developer upon whom they reasonably relied "took affirmative steps to conceal material facts" about a real estate transaction from the plaintiffs. Plaintiffs have presented no evidentiary materials that could be construed in any fashion to support a theory that Lenovo took affirmative steps to conceal material facts. The actual facts show as soon as Lenovo became aware of the alleged "serious cybersecurity flaw," Lenovo diligently presented significant information to the public about the issue. *See* notes 21-27 *supra*.

favor of defendant on UDTPA claim where plaintiff could not show "that [defendant] engaged in immoral, unethical, oppressive, or substantially injurious trade practices").[46] Thus Plaintiffs fall well short of carrying their burden.

IV. AN INJUNCTION REQUIRING INDIVIDUAL NOTICE ACCOMPLISHES LITTLE, AND WOULD BE EXTRAORDINARILY BURDENSOME.

"A preliminary injunction is an extraordinary remedy never awarded as of right. . . In each case, courts 'must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief.'" *Winter*, 555 U.S. at 24 (quoting *Amoco Prod. Co. v. Vill. of Gambell*, 480 U.S. 531, 542 (1987)). In this case, the burden on Lenovo to perform the requested relief far exceeds any potential value in issuing the requested injunctive relief at this stage of the litigation.

It is impossible for Lenovo to identify (much less actually reach and notify by mail and e-mail) all individuals who possess an Affected Machine. The names and contact information of purchasers are often not made known to Lenovo because many customers purchased their machines from third-party retailers (such as Best Buy and Tiger Direct) that do not report the names to Lenovo. Lenovo is only aware of a small percentage of purchasers from other retail stores, generally only because those customers participated in a Lenovo rebate program or voluntarily registered their product with Lenovo. It would be impossible for Lenovo to ascertain all the names of those purchasers, much less their current contact information. Even an attempt to locate the names and current contact information of individuals who have become known to Lenovo at some point in time would be burdensome and time-consuming. Not only is searching out the identity of each purchaser

[46] Plaintiffs' UDTPA claims for another reason as well: as discussed in Section II.A. *supra*, they have not pled or shown that they were proximately injured by any action of Lenovo. *See Kelley v. Enviva, L.P.*, No. 7:14–CV–126–BO, 2015 WL 500473 at *4 (E.D.N.C. Feb. 4, 2015) (citing *Nucor Corp. v. Prudential Equity Grp., LLC*, 189 N.C. App. 731, 738, 659 S.E.2d 483, 488 (2008)) ("[P]roximate cause is a required element of a UDTPA claim."); *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203–04 (9th Cir. 2010) (citing *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959–60 (9th Cir. 2009) (finding that in order to succeed on UCL claim, a plaintiff must show that (1) he or she has suffered actual injury in fact, and (2) such injury occurred as a result of the defendant's alleged unfair competition).

expensive and impractical, but even attempting to do so on a "best efforts" basis would be impossible to implement and would invite disagreement and controversy as to what "best efforts" means.

The potential "benefit" of issuing the mandatory injunctive relief requested is quite marginal. The best information available to Lenovo suggests that less than 10-20% of all purchasers of Affected Machines have not utilized a tool to have the Software removed from the Affected Machines: the other 80-90% of individuals with an Affected Machine have already removed the Software by one of the many mechanisms Lenovo has made available. Hunt Decl. ¶4. Mandating that Lenovo extensively search all of its records and the records of third-parties not under its control to locate the names and current contact information of any individuals with whom Lenovo sold an Affected Machine would be burdensome and time-consuming. It would unnecessarily duplicate the more efficient and effective means that Lenovo has used to notify users about any issues with the Software.

V. THE RELIEF REQUESTED DOES NOT SERVE THE PUBLIC INTEREST.

Given that Plaintiffs have not demonstrated any actual harm or imminent threat of harm should the Court deny its request for mandatory preliminary relief, no strong public interest weighs in favor of the relief requested. There is, however, a significant public interest in promoting the "just and efficient" use of court resources and avoiding the risk of "inconsistent outcomes" by denying the injunction (or at minimum, delaying a ruling on the injunction) until the JPML issues a decision on whether multiple actions across the country should be consolidated in front of a single judge. *See Hertz Corp. v. The Gator Corp.*, 250 F. Supp. 2d 421, 428 (D.N.J. 2003) (granting defendants' motion to stay pending a Multi-District Litigation ("MDL") decision before ruling on plaintiff's motion for preliminary injunction and finding "considerations of judicial economy" weigh against potential harm to plaintiff and in favor of a stay); *JBR, Inc. v. Keurig Green Mountain, Inc.*, No. 2:14-cv-00677-KJM-CKD, 2014 WL 1767701 *2 (E.D. Cal. May 2, 2014) (granting defendant's

motion to stay proceedings pending an MDL decision and finding considerations of judicial economy to weigh in favor of the stay).

To date, 25 similar lawsuits have been filed in federal courts throughout the country by plaintiffs purporting to bring class actions on behalf of purchasers of Lenovo computers containing the Software (collectively, including this action, the "*Lenovo Adware Litig.* cases"). A motion is pending before the JPML to transfer the *Lenovo Adware Litig.* cases for coordinated and consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 ("MDL Motion"). *MDL No. 2624, IN RE: Lenovo Adware Litigation*. The MDL Motion has not yet been set for hearing before the JPML. All parties have agreed to MDL consolidation, and the only issue in the MDL Motion to be decided is the appropriate venue.

As in *Hertz* and *JBR*, the strong public interest in promoting judicial economy and consistent case outcomes weighs in favor of denying (or at least delaying a decision on) Plaintiffs' extraordinary request for a mandatory injunction until the JPML can decide the ultimate venue in which this case will reside. By doing so, the District Court judge deciding the merits of the case will have "the opportunity to become familiar with the technology at issue and evaluate the facts, rendering consistent pretrial decisions in all of the consolidated actions based upon that more thorough understanding." *Hertz*, 250 F. Supp. 2d at 428.

CONCLUSION

For the reasons stated hereinabove, Lenovo respectfully requests that the Court deny Plaintiffs' Motion for Preliminary Injunction.

Respectfully submitted, this 3rd day of April, 2015.

WOMBLE CARLYLE SANDRIDGE & RICE, LLP

/s/ Hayden J. Silver

Hayden J. Silver III (NC State Bar # 10037)
Email: jsilver@wcsr.com
Betsy Cook Lanzen (NC State Bar # 25353)
Email: blanzen@wcsr.com
Raymond M. Bennett (NC State Bar # 36341)
Email: rbennett@wcsr.com
150 Fayetteville St., Suite 2100
Raleigh, North Carolina 27601
Phone: (919) 755-2188
Fax: (919) 755-6099
Attorneys for Lenovo (United States) Inc.

DYKEMA GOSSETT PLLC

/s/ Daniel J. Stephenson

Daniel J. Stephenson (CA State Bar No. 270722)
Email: Dstephenson@dykema.com
333 South Grand Avenue, Suite 2100
Los Angeles, CA 90071
Phone: (213) 457-1780
Fax: (855) 223-7056

Attorneys for Lenovo (United States) Inc.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing **DEFENDANT LENOVO'S OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION** with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following:

Stephen McDaniel Russell, Jr.
Van Laningham Duncan PLLC
300 N. Greene Street, Suite 850
Greensboro, NC 27401
srussell@vldlitigation.com

Alan W. Duncan
Van Laningham Duncan PLLC
300 N. Greene Street, Suite 850
Greensboro, NC 27401
aduncan@vldlitigation.com

Joel A. Fleming
Block & Leviton LLP
155 Federal Street, Suite 400
Boston, MA 02110
Joel@blockesq.com

Jason M. Leviton
Block & Leviton LLP
155 Federal Street, Suite 400
Boston, MA 02110
Jason@blockesq.com

This the 3rd day of April, 2015.

/s/ Hayden J. Silver, III __
Hayden J. Silver III (NC State Bar No. 10037)
Email: jsilver@wcsr.com
150 Fayetteville Street, Suite 2100
Raleigh, North Carolina 27601
Phone: (919) 755-2188
Fax: (919) 755-6099

Attorney for Lenovo (United States) Inc.